PRIVACY IMPACT ASSESSMENT

Enterprise Payment Service (EPS)

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) **Name of system:** Enterprise Payment Service

(b) **Bureau:** Consular Affairs (CA)

(c) **System acronym**: EPS

(d) **iMatrix Asset ID Number:** 260640

(e) **Reason for performing PIA**:

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

The initial Assessment and Authorization process is underway and EPS is expected to receive an Authorization-To-Operate by August 31, 2017.

(c) Describe the purpose of the system:

The Enterprise Payment Service (EPS) is a building block of the Consular Shared Tables (CST) Enterprise Architecture that will provide a standards-based, extensible and reusable payment collection capability to CST applications that need to collect fees for services from their consumers. The service will use pay.gov's Trusted Collection Service (TCS) as the underlying payment service provider. The pay.gov web-based application is owned and operated by the Department of Treasury. EPS will cater to two types of consumers within the CST application portfolio. These include web applications that are invoked from a user's browser, and client-server applications that involve the use of peripherals such as a Point of Sale (POS) credit-card terminal.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

- Payment Account Name (First, Last and Middle Initial)
- Payment Account Holder Personal Address
- Pay.gov activity report; stored to support settlement inquiries and will contain a masked account number (last 4 digits of a credit card)

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. § 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. § 1185 (Travel Control of Citizens)
- 18 U.S.C. §§ 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. §§ 211a-218, 2705 Passports and Consular Reports of Birth Abroad (CRBAs)
- 22 U.S.C. § 2651a (Organization of Department of State), Executive Order 11295, August 5, 1966, 31 FR 10603; (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 U.S.C. § 3927 (Chief of Mission)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 U.S.C. § 6039E (Information Concerning Resident Status)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(f) **Is the information searchable by a personal identifier (e.g., name or Social Security number)?**

☒**Yes, provide:**

- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

State-05 Overseas Citizens Services Records and Other Overseas Records, September 8, 2016
State-26 Passport Records, March 24, 2015

Note: The purpose of the system is not for searching data. However, if there is a successful connection to the EPS database any data in any EPS table may be queried within the EPS schema. No EPS Web Service will permit the search of a previously submitted payment transaction based upon a person or organization's billing information (name, address, bank account number, etc.).

☐No, explain how the information is retrieved without a personal identifier.

(g) **Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?** ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) **Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?** ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

Schedule number Department of State Records Disposition Schedule:

A-13- Passport Records
Length of time the information is retained in the system:
The length of time a record will be kept is dependent on the specific item and the applicable rules in A-13-001 of the State Department records retention schedule. Specific information may be found at this link: http://infoaccess.state.gov/recordsmgt/recdispsched.asp.

Type of information retained in the system: It should be noted that prior to 1999, records of some data were stored in microfilm or silver halide. Records in the systems are files associated with a U.S. citizen applying for and receiving, or being denied, a U.S. passport.

A-15-001-02 through 4c Overseas Citizens Records
Length of time the information is retained in the system:
The length of time a record will be kept is dependent on the specific item and the applicable rules in A-15-001 of the State Department records retention schedule. Specific information may be found at this link: http://infoaccess.state.gov/recordsmgt/recdispsched.asp.

Type of information retained in the system: It should be noted that prior to 1999, records of some data were stored in microfilm or silver halide. Records in the systems are files associated with a U.S. citizen applying for and receiving, or being denied, a U.S. passport and/or a CRBA and other overseas citizen's services.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public (are U.S. citizens or aliens lawfully admitted for permanent residence)
☐ U.S. Government/Federal employees or Contractor employees
☒ Other (are not U.S. citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security numbers (SSNs), is the collection necessary?

☐Yes ☒No (SSNs are not collected)

- If yes, under what authorization?

(c) How is the information collected?

U.S. citizen:
Individuals seeking to renew their passport online would go to the public facing website. At the point where payment for the passport renewal will be paid, EPS directs the individual to pay.gov. The payment is made and applicant is directed back to EPS. An electronic receipt is created. EPS retains only the first and last name, last 4 digits of the credit card number, and address. As EPS evolves, the process will be the same for any payment EPS processes.

Others:
The information is collected directly from the customer who is requesting a fee-based consular service. This information is either manually entered or automatically collected when the credit card is swiped.

(d) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other
- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?
It is up to the individual entering the information to ensure that the information is accurate. Pay.gov checks the accuracy of payment information such as card number.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Data is maintained as current by virtue of data checks and applicant input into the system where application is entered (i.e., Consular Electronic Application Center (CEAC)). Mismatched data checks are resolved before the passport renewal or Consular Report of Birth Abroad (CRBA) application moves forward for payment.

(g) Does the system use information from commercial sources? Is the information publicly available?
No. EPS does not use commercial or publicly available information.

(h) Is notice provided to the individual prior to the collection of his or her information?

Yes, notice is provided to the individual; when the applicant applies for a passport renewal, the collection system provides the notice.

(i) **Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?** ☒Yes ☐No

- If yes, how do individuals grant consent?

The consent is provided by the collection system; for example, CEAC & ACRS (Automated Cash Register System).

No, EPS: EPS is not a customer-facing application and therefore will not interface directly with customers paying for consular services. EPS is a service accessed by other systems.

Yes, ACRS: an individual does have the opportunity or right to decline to provide information. However, if he or she declines, he/she will not be provided with the consular service requested (e.g. a passport).

Yes, CEAC: An applicant voluntarily elects to complete the visa application process, and all associated CEAC forms. The forms notify the applicant regarding the type of information to be collected, justification for the collection, routine uses, potential sharing arrangements, data protection measures, and the consequences of not providing the data.

Visa applications display a statement that the information is protected by section 222(f) of the INA. Section 222(f) provides that records pertaining to the issuance and refusal of visas shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

- If no, why are individuals not allowed to provide consent? N/A

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII items listed in Question 3d are the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were cogitated during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function for which it was intended.

5. Use of information

(a) What is/are the intended use(s) for the information?

The intended use of the information is to facilitate the passport renewal process by providing a simplified payment method.

(b) **Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?**

Yes. The PII is used according to the stated purpose for the design.

(c) **Does the system analyze the information stored in it?** ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?
N/A

(2) **Does the analysis result in new information?**
☐Yes ☒No

(3) **Will the new information be placed in the individual's record?**
☐Yes ☒No

(4) **With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it**?
☐Yes ☒No

6. Sharing of Information

(a) **With whom will the information be shared internally and/or externally? Please identify the recipients of the information**.

Information will be shared internally with CA systems ACRS and CEAC. Externally, information will be shared with pay.gov for the purpose of processing a payment for consular services such as a passport renewal or a CRBA application.

EPS is not a customer-facing application and therefore will not interface with customers paying for consular services. EPS is a service accessed by other systems**.**

(b) **What information will be shared**?

Name, address, and credit card will be shared (credit card is not persistent; only the last 4 digits will be saved).

(c) What is the purpose for sharing the information?

The information is shared in order to process payments for passport renewals or CRBA applications.

(d) The information to be shared is transmitted or disclosed by what methods?

All exchanges between agency applications and EPS and between EPS and pay.gov, will be transmitted via secured electronic methods approved by the Department of State.

(e) What safeguards are in place for each internal or external sharing arrangement?

The information transmitted will be secured using transport security as well as encryption. Agreements are in place for ACRS and CEAC; each application sets up a pay.gov "agency" which defines the relationship.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

a. Accidental disclosure of information to non-authorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles or authorization, and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.
b. Deliberate disclosure/theft of information regardless of whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, “Sensitive but Unclassified”, and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization and need-to-know

- System authorization and accreditation process along with continuous monitoring (Risk Management Framework). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications shared with external agencies are encrypted as per the Department of State’s security policies and procedures.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Applicants do not have access to their information directly on the system; however, procedures for notification and redress are published in the Privacy Act System of Records Notice (SORN) State-05 Overseas Citizens Services Records and Other Overseas Records and State-26 Passport Records. In addition, procedures are published on the Department of State public website.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.
Individuals cannot correct information directly in EPS. EPS accepts the transaction from ACRS and CEAC. The only way information can be changed is through ACRS and CEAC.

(c) **By what means are individuals notified of the procedures to correct their information?**
Information cannot be corrected in EPS. Individuals wishing to correct information must access ACRS or CEAC. The procedures for correcting information in those systems are detailed in their respective PIAs.

8. Security Controls

(a) How is the information in the system secured?
The system is secured within the Department of State intranet where risk factors are mitigated through the use of defense in-depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

Access to applications is controlled at the application level; there are additional access controls at the database level. All accounts for the system must be approved by the user's supervisor and the Information System Security Officer. The audit vault system is used to monitor all privileged access to the system and violations are reported to senior management daily, if applicable. Data shared with the Department of Treasury is carefully regulated according to a Memorandum of

Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by the Authorizing Officers of each agency.

Applications are configured according the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable NIST 800-53 (National Institute of Standards and Technology) and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

To access the system, persons must be authorized users of the Department of State's unclassified network, which requires a background investigation and an application approved by the supervisor and Information System Security Officer (ISSO). Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a PIV/CAC and PIN (Personal Identify Verification/Common Access Card and Personal Identification Number) which meets the dual authentication requirement for federal system access and is required for logon.

In addition to the PIV/CAC and PIN, the user's account requires the password be changed on a recurring basis. If the password expires, the account is locked. If a user does not log in for two months, the account is deactivated.

A system use notification ("warning banner") is displayed before logon is permitted and informs the user of system use and restrictions with every login. Users are required to read and actively click a button indicating understanding and agreement before logon can be completed.

Access to the system is role based and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with DS configuration guides, and conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain

compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the Department's OpenNet-connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g. administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with DS Security Configuration guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with DS configuration guides, auditing is enabled to track the following events on the host operating systems and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

Operating System-Level auditing is set in accordance with the DS Security Configuration Guide. The OS (Operating System) interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. In addition to the security log, the system log and application logs provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures

- Restart/shutdown/system security – successes and failures
- Process tracking – failure

(d) **Explain the privacy training provided to the authorized users of the system.**
In accordance with Department of State computer security policies, mandatory annual security/privacy training is required for all authorized users including regular refresher training. Each user must complete the Cyber Security Awareness Training annually. Users must also take the Privacy PA-459 course, entitled Protecting Personally Identifiable Information. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) **Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?** ☒Yes ☐No
If yes, please explain.
To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted; physical and environmental protection is implemented; media handling configuration management is utilized; and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) How were the security measures above influenced by the type of information collected?
Security measures were influenced by being aware that the consequence to organizations or individuals whose PII has been breached or exposed to unauthorized users may include inconvenience, distress, or damage to standing or reputation, financial loss, harm to Department programs or the public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violation. The security measures listed above were implemented to secure the data in the system.

9. Data Access

(a) **Who has access to data in the system?**

System Administrators are responsible for all daily maintenance, establishing access control lists (ACLs), and backups. The duties of system administrators require that they be granted system

administrator privileges to the respective application servers. The respective post representative authorizes the establishment, activation, modification, review, disabling, and removing of all System Administrator accounts.

Database Administrators (DBA) are responsible for the daily maintenance, upgrades; patch/hot fix application, backups and configuration, to the database. DBA access is controlled by the Integrated Services (IS) team through the use of ACLs as established by the system administrators. This System DBAs are authenticated using Windows operating system authentication. The CA ISSO is responsible for reviewing and approving DBA accounts.

In addition, all State Department users must complete and agree to an acknowledgement agreement form, acknowledge the Security Awareness Training procedures, sign the rules of behavior issued before access is given to the OpenNet and respective applications; and sign the nondisclosure agreements, acceptable use agreements and conflict-of-interest agreements that are also discussed and explained to the users before access is given to any CA/CST system.

Once the highest-level background investigation available has been completed, cleared technical personnel (government and contractors) will be allowed to access the server rooms housing the respective applications. In addition, all domestic CA positions are reviewed for sensitivity level.

(b) **How is access to data in the system determined?**
Access is determined based on requests which are approved by the supervisor and ISSO. Access is role based and user is granted only the role(s) required to perform officially assigned duties.

(c) **Are procedures, controls or responsibilities regarding access to data in the system documented?** ☒Yes ☐No
Information is documented in the System Security Plan. The Plan includes information regarding system access to data.

(d) **Will all users have access to all data in the system, or will user access be restricted? Please explain.**
Users will not have access to all data in the system outside of administrators. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

(e) **What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?**

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented.

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN).